(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 June 2005 (09.06.2005)

PCT

(10) International Publication Number
WO 2005/053262 A1

(51) International Patent Classification[7]: H04L 29/06, 12/58

(21) International Application Number: PCT/EP2004/052907

(22) International Filing Date: 10 November 2004 (10.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03368104.0 27 November 2003 (27.11.2003) EP

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; IBM Corporation, New Orchard Road, Armonk, New York 10504 (US).

(71) Applicant *(for MC only)*: **COMPAGNIE IBM FRANCE** [FR/FR]; Tour Descartes, La Defense 5, 2 Avenue Gambetta, F-92400 COURBEVOIE (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **COLLET, Jean-Luc** [FR/FR]; 698 route de St Jeannet, F-06610 La Gaude (FR). **DROUET, François Xavier** [FR/FR]; Cap Fabron - "LE Flore" 2bis, bd Montreal, F-06200 NICE (FR). **MARMIGERE, Gerard** [FR/FR]; Quartier Le Patrimoine, F-06340 DRAP (FR). **PICON, Joaquin** [FR/FR]; Riviera Baie, 240, ave Paul Cezanne, F-06700 St Laurent du Var (FR).

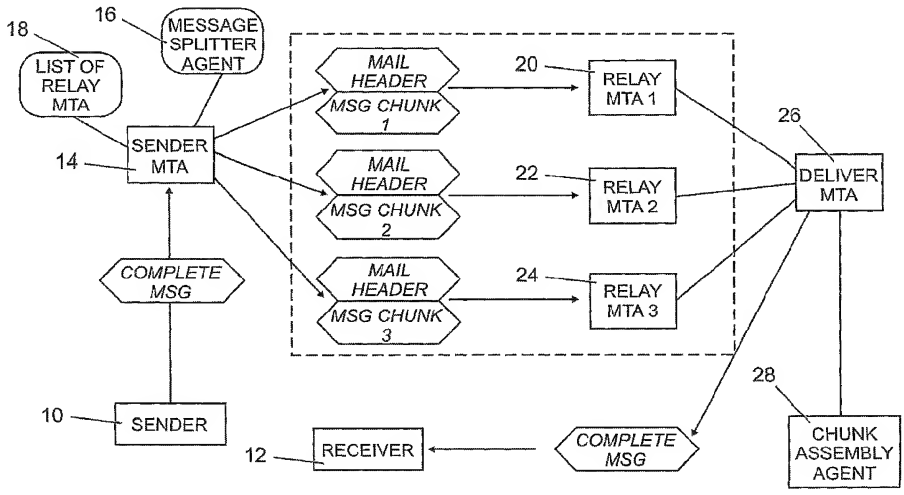
(74) Agent: **ETORRE, Yves, Nicolas**; Compagnie IBM France, Intellectual Property Department, F-06610 La Gaude (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH,

[Continued on next page]

(54) Title: SYSTEM FOR ENHANCING THE TRANSMISSION SECURITY OF THE E-MAILS IN THE INTERNET NETWORK



(57) Abstract: System for enhancing the security of the e-mails transmitted from a sender (10) to a receiver (12) over a data transmission network such as Internet wherein a Message Transfer Agent (MTA) (14) associated with the sender is in charge of transmitting over the network an original e-mail sent by the sender. The MTA associated with the sender includes a message splitting means (16) adapted to divide the original e-mail into a plurality of chunks according to a predetermined algorithm and a predetermined list of relay MTAs (20, 22, 24) to which are forwarded the plurality of chunks. The system comprises a chunk assembly agent (28) for receiving from the relay MTAs the plurality of chunks and re-assembling them by using the predetermined algorithm in order to re-build the e-mail before sending it to the receiver.

WO 2005/053262 A1

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM FOR ENHANCING THE TRANSMISSION SECURITY OF THE E-MAILS IN THE INTERNET NETWORK

Technical field of the invention

The present invention relates to the security in the transmission of the e-mails over an unsecured data transmission network and in particular relates to a system for enhancing the transmission security of the e-mails in the Internet network.

Background art

Today, the use of e-mails is widely spread. When the sender forwards an e-mail to a recipient, the action is immediate and unless a problem is encountered between the sender server and the recipient server, the e-mail is delivered in the recipient mailbox without any control on the way taken by the forwarded message in terms of network infrastructure.

Most countries have specific legal protections that prevent authorities and individuals from opening and reading the paper mail. Unfortunately, few countries have provided the same protections for the electronic mail, which gives individuals, companies and authorities a legal room to read the e-mails. Thus, the e-mails can be read at any of the routers along the path taken by the e-mail to reach its destination over the Internet. However, due to the growth of commercial and private contracts materialized by the electronic mail, it becomes crucial to be able to guarantee privacy of such exchanges.

To prevent attacks of e-mails, the usage of encryption algorithms either symmetric or asymmetric to secure the e-mail exchange over the Internet is widely spread. Thus, in the key

encryption, there is a private key kept private for the owner, which is used to sign the data whereas a public key which can be known of many people is used for decrypting the message. To improve the security, such keys have a minimum of 40 bits but are longer and longer. For example, the symmetric algorithm Data Encryption Standard specifies 56-bit keys in some countries and 128-bit keys in other ones like the USA. Therefore, there is no doubt that such a continuous growth of the key length is not a solution for the security problem.

Summary of the invention

Accordingly, the object of the invention is to provide a system and to achieve a method which can be adapted to any kind of e-mail being transmitted over the Internet network without requiring the use of sophisticated algorithms and/or more and more long encryption keys.

The invention therefore relates to a system for enhancing the security of the e-mails transmitted from a sender to a receiver over a data transmission network such as Internet wherein a Message Transfer Agent (MTA) associated with the sender is in charge of transmitting over the network an original e-mail sent by the sender. The MTA associated with the sender includes a message splitting means adapted to divide the original e-mail into a plurality of chunks according to a predetermined algorithm and a predetermined list of relay MTAs to which are forwarded the plurality of chunks. The system comprises a chunk assembly agent for receiving from the relay MTAs the plurality of chunks and re-assembling them by using the predetermined algorithm in order to re-build the e-mail before sending it to the receiver

Brief description of the drawings

The above and other objects, features and advantages of the invention will be better understood by reading the following more particular description of the invention in conjunction with the accompanying drawings wherein:

- Fig. 1 is a schematic representation of a system according to the invention wherein an e-mail is divided into three chunks using three different paths over Internet; and
- Fig. 2 is a diagram representing the original e-mail divided into five chunks distributed among three different e-mails.

Detailed description of the invention

In reference to FIG.1, in the system according to the invention, it is assumed that a sender 10 wants to send an e-mail to a receiver 12 over the public data transmission network, that is Internet, represented inside the dotted lines in the figure.

The e-mail MSG sent by the sender 10 can be encrypted by the public key of the receiver 12 even though this is not mandatory. The e-mail MSG preferably encrypted is then provided for transmission to the associated Message Transfer Agent (MTA) 14 after adding a mail header such as the e-mail COMPLETE MSG to be forwarded is as follows:

```
To : receiver@dest.domain
From : sender
Subject : secure mail
ENCRYPTED TEXT
```

wherein receiver@dest.domain is the address of the receiver mailbox. It must be noted that this address is in clear

insofar as the sender MTA 14 is a secure zone that can be the Intranet network of a company or the client device of a standalone user.

The sender MTA 14 includes two essential means according to the invention : a message splitter agent 16 and a list of relay MTAs 18. The message splitter agent 16 is in charge of dividing the received e-mail COMPLETE MSG into a plurality of chunks and to encrypt each chunk with its mail header by using the public key of a specific mailbox having the address highlysecure@dest.dom. Each new e-mail MSG CHUNK is as follows:

To : receiver@dest.domain
From : sender
Subject : secure mail
Chunk : n
Chunk count : N

A same MAIL HEADER is added to each encrypted chunk before sending it over the Internet network. This MAIL HEADER is as follows :

To highlysecure@dest.domain
From : Confidential
Subject : xxx

By using its list of relay MTAs 18, the sender MTA 14 forwards each encrypted chunk with its header to a different relay MTA. Thus, in the example illustrated in FIG.1, the e-mail is divided into three e-mails forwarded to the relay MTAs 20, 22 and 24. Thus, sending a plurality of chunks to respectively a plurality of MTAs ensures a different pathway for each chunk while they transit over the unsecured public network. It must

be noted that such a division into chunks can depend on the security level required by the sender.

Since all the chunk e-mails have the same destination address highlysecure@dest.domain, they are received by a single deliver MTA 26 associated with this address. Then, the deliver MTA sends the received chunk e-mails to the mailbox corresponding to the address highlysecure@dest.domain which is a chunk assembly agent 28. By using its private key, the chunk assembly agent 28 decrypts each received e-mail and can re-assemble the plurality of received chunks by using the same algorithm which has been used by the message splitter agent to divide the original e-mail into a plurality of chunks, the chunk number n included in the header being used to concatenate the chunks in the right order even if they have been received in a different order.

Finally, the original message COMPLETE MSG which has been obtained after re-assembling the chunks in the chunk assembly agent 28, is forwarded to the mailbox of the receiver 12 by the deliver MTA 26.

The scrambling algorithm used to divide the original e-mail into a plurality of chunks may be any kind of algorithm. But as mentioned above, it is essential that the chunk assembly agent uses the same algorithm to re-assemble the e-mail as the one used by the message splitter agent to divide the e-mail into chunks.

For instance, it can be assumed that each chunk is composed of the same number of n bytes. Assuming that there are m relay MTAs, the original e-mail could be divided in the following way:

Bytes from 1 to n in chunk #1 for the first relay MTA
Bytes from n+1 to 2n in chunk #2 for the second relay MTA

Bytes from 2n+1 to 3n in chunk #3 for the third relay MTA

- - - - -

Bytes from mn+1 to (m+1)n in chunk #m+1 for the m^{th} relay MTA

Bytes from (m+1)n+1 to (m+2)n in chunk #m+2 for the first relay MTA

Bytes from (m+2)n+1 to (m+3)n in chunk #m+3 for the second relay MTA

- - - - -

According to another more secure embodiment, the original e-mail may be divided at the character level. A possible algorithm consists in taking sequentially each character and put it in a chunk the number of which is defined by the following formula used with X chunks:

Chunk # = 1 + <order number of the character> *modulo X*

Assuming that the message is "DIVIDE THE MESSAGE" and that the characters are put into 5 chunks, the chunks are the following:

Chunk 1 DE A
Chunk 2 I MG
Chunk 3 VTEE
Chunk 4 IHS
Chunk 5 DES

Then, the chunks could be distributed randomly into the different e-mails forwarded to the relay MTAs.

Thus, assuming that there are three relay MTAs as described in FIG.1, the original e-mail could be divided into 5 chunks as illustrated in FIG.2. In such a case, chunk #1 and chunk #4 are included in the e-mail forwarded to relay MTA 20, chunk #2 and chunk #5 are included in the e-mail forwarded to relay MTA 22 and chunk #3 is forwarded to relay MTA 24. It must be noted that each chunk is preceded, in each e-mail, by the chunk

number in order for the chunk assembly agent 28 to be able to re-assemble correctly the original e-mail even though the partial e-mails are not received in the right order.

CLAIMS

1. System for enhancing the security of the e-mails transmitted from a sender (10) to a receiver (12) over a data transmission network such as Internet wherein a Message Transfer Agent (MTA) (14) associated with said sender is in charge of transmitting over said network an original e-mail sent by said sender;

   said system being characterized

   in that said MTA associated with said sender includes a message splitting means (16) adapted to divide said original e-mail into a plurality of chunks according to a predetermined algorithm and a predetermined list of relay MTAs (20, 22, 24) to which are forwarded said plurality of chunks; and

   in that it comprises a chunk assembly agent (28) for receiving from said relay MTAs the plurality of chunks and re-assembling them by using said predetermined algorithm in order to re-build said e-mail before sending it to said receiver.

2. The system according to claim 1, wherein each of said plurality of chunks is transmitted as a chunk e-mail having a destination address which is the address of said chunk assembly agent (28).

3. The system according to claim 2, wherein each of said plurality of chunks is encrypted by using the public key of said chunk assembly agent (28) before being transmitted over said network.

4. Method for enhancing the security of the e-mails transmitted from a sender (10) to a receiver (12) over a data transmission network such as Internet wherein a Message Transfer Agent (MTA) (14) associated with said sender is in charge of transmitting an original e-mail sent by said sender;

said method being characterized in that it consists in using an algorithm for dividing said original e-mail into a plurality of chunks, and sending these chunks as e-mails to different relay MTAs (20, 22, 24) defined in a predetermined list of relay MTAs, re-assembling by a chunk assembly agent said chunks in order to re-build said original e-mail by using said predetermined algorithm, before sending said original e-mail to said receiver.

5. The method according to claim 4, wherein each chunk is transmitted over said network in a chunk e-mail having a destination address which is the address of said chunk assembly agent.

6. The method according to claim 4, wherein each chunk is encrypted by using the public key of said chunk assembly agent before being transmitted, said encrypted chunk e-mail being decrypted when received by said chunk assembly agent using its private key.

7. The method according to claim 6, wherein the text of said original e-mail is encrypted by using the public key of said receiver before being divided into a plurality of chunks.

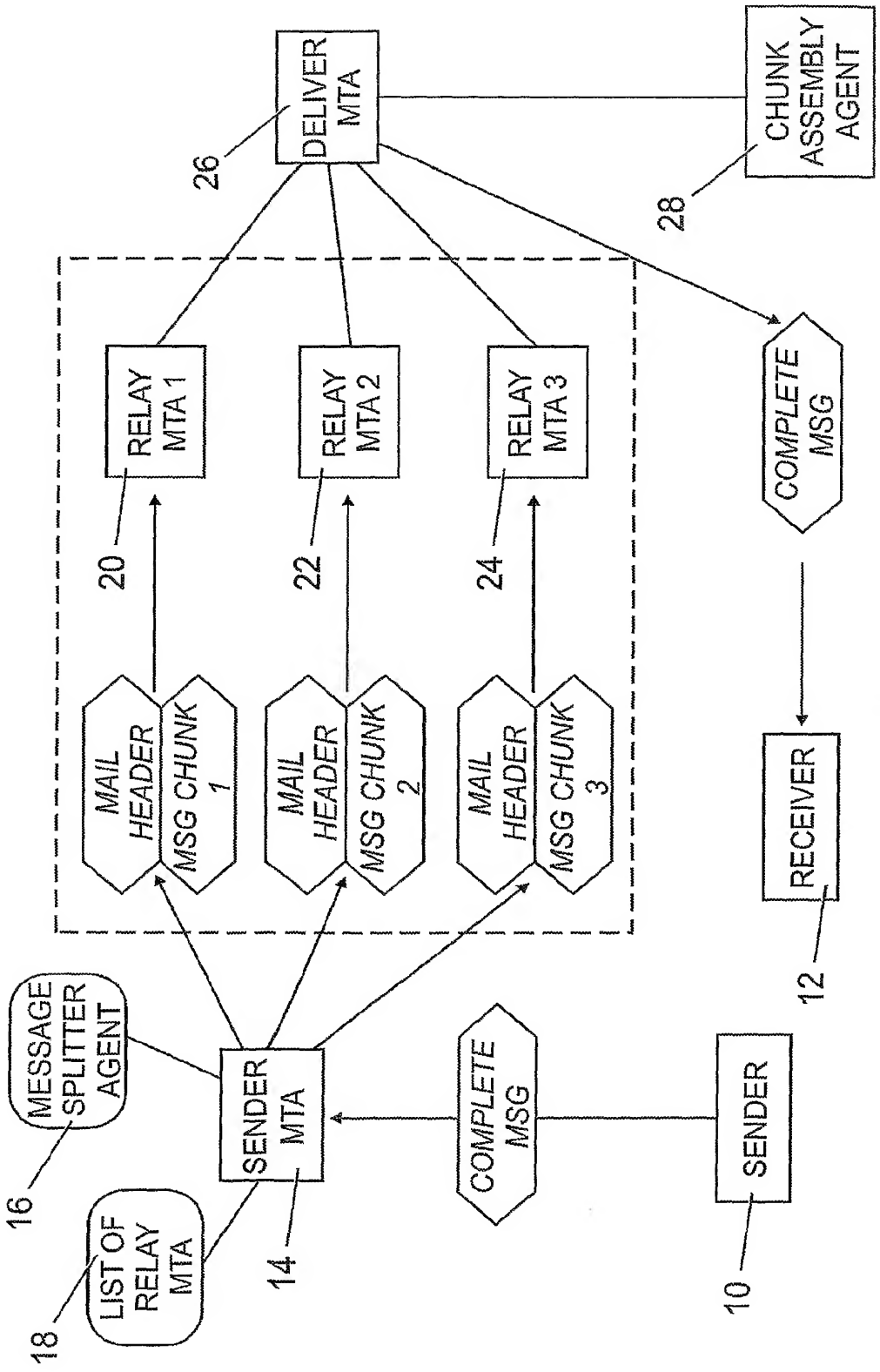

SENDER
10
SENDER MTA
14
MESSAGE SPLITTER AGENT
16
LIST OF RELAY MTA
18
RELAY MTA 1
20
RELAY MTA 2
22
RELAY MTA 3
24
DELIVER MTA
26
CHUNK ASSEMBLY AGENT
28
RECEIVER
12
COMPLETE MSG
COMPLETE MSG
MAIL HEADER
MSG CHUNK 1
MAIL HEADER
MSG CHUNK 2
MAIL HEADER
MSG CHUNK 3

Fig. 1

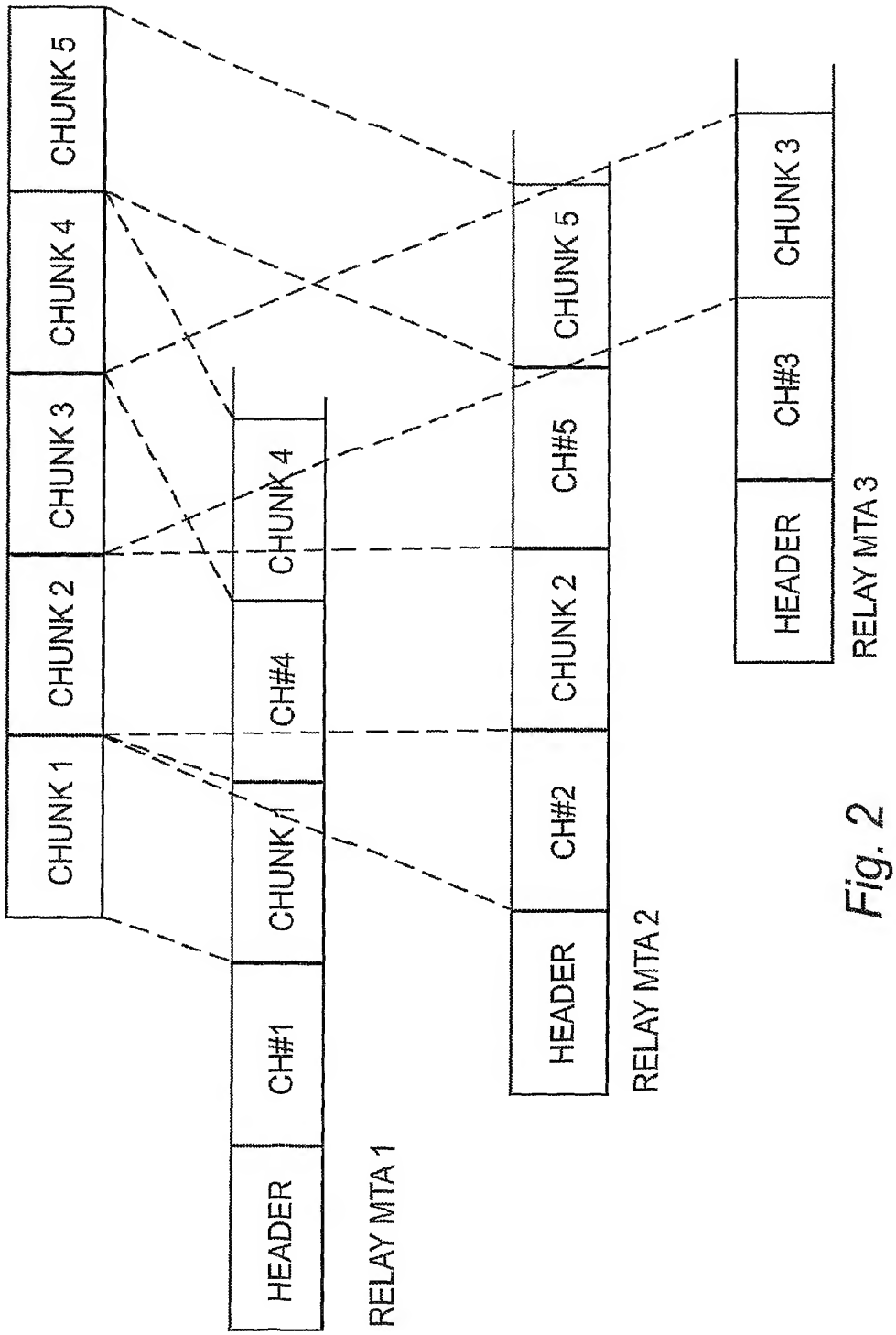

CHUNK 1
CHUNK 2
CHUNK 3
CHUNK 4
CHUNK 5
HEADER
CH#1
CHUNK 1
CH#4
CHUNK 4
RELAY MTA 1
HEADER
CH#2
CHUNK 2
CH#5
CHUNK 5
RELAY MTA 2
HEADER
CH#3
CHUNK 3
RELAY MTA 3

Fig. 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/052907

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/101339 A1 (BIANCHINI PAOLO ET AL) 29 May 2003 (2003-05-29) abstract paragraph '0015! - paragraph '0017! paragraph '0022! - paragraph '0024! paragraph '0035! - paragraph '0043! figures 2a,2b	1-7
X	US 2003/167314 A1 (GILBERT MARTYN ET AL) 4 September 2003 (2003-09-04) paragraph '0059! - paragraph '0060! paragraph '0081! - paragraph '0108! paragraph '0117! - paragraph '0120! paragraph '0129! - paragraph '0139! paragraph '0150! - paragraph '0152! paragraph '0162! paragraph '0175! - paragraph '0177!	1-7

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 February 2005	02/03/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Apostolescu, R

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/052907

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/112008 A1 (CHRISTENSON NIKOLAI PAUL ET AL) 15 August 2002 (2002-08-15) paragraph '0015! - paragraph '0020! paragraph '0257! - paragraph '0298!	1-7

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/052907

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003101339 A1	29-05-2003	NONE	
US 2003167314 A1	04-09-2003	GB 2363948 A	09-01-2002
		AU 2016701 A	02-01-2002
		AU 7424301 A	02-01-2002
		AU 7426401 A	02-01-2002
		WO 0199379 A1	27-12-2001
		GB 2363949 A	09-01-2002
		WO 0199380 A1	27-12-2001
		WO 0199381 A1	27-12-2001
US 2002112008 A1	15-08-2002	NONE	